UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

STEPHEN NICK and MATTHEW DASH, Individually And On Behalf of All Others Similarly Situated Plaintiffs, - against - TARGET CORPORATION, Defendant.	Jury Trial Demanded Case No. 15-cv-4423 Hon. Leonard D. Wexler, U.S.D.J. Hon. Gary R. Brown, U.S.M.J.

FIRST AMENDED CLASS ACTION COMPLAINT

Plaintiffs Stephen Nick and Matthew Dash, for their first amended class action complaint on behalf of themselves and all others similarly situated, upon personal knowledge as to the facts pertaining to them and upon information and belief as to all other matters, based on investigation of their counsel, against defendant Target Corporation, state as follows:

NATURE OF ACTION

1. This is a consumer class action for damages and injunctive relief arising from Defendant's deceptive and unlawful conduct in illegal and surreptitious collection and use of personal information from drivers' records of purchasers of certain items at Defendant's retail stores.

2. Although Defendant is a retailer, it behaves in many respects as a high tech company. Indeed, Target has one of the top forensics labs in the country far surpassing the capabilities of many law enforcement agencies. *See* Sarah Bridges, *Retailer Target Branches Out Into Police Work*, THE WASHINGTON POST (Jan. 29, 2006), http://www.washingtonpost.com/wp-dyn/content/article/2006/01/28/AR2006012801268.html.

3. Defendant also admits to purchasing raw data in order to predict consumer behavior and direct coupons and targeted advertisement at its guests. *See* Kashimir Hill, *How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did*, FORBES (Feb. 16, 2012, 11:02 AM), http://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/#f7a70e634c62; *see also* Charles Duhigg, *How Companies Learn Your Secrets*, NEW YORK TIMES (Feb. 16, 2012), http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=1&_r=1&hp.

4. On information and belief, this raw data includes motor vehicle records, which Defendant purchases from various state department of motor vehicles in bulk. *See* http://help.target.com/help/subcategoryarticle?childcat=Accepted+payment+methods&parentcat=Payment+Methods (accessed on Jan. 29, 2016) (Target accepts personal checks); *see also* VII Business Torts, 3-33, *Privacy and Publicity: Intrusion Upon Seclusion*, § 33.02 (Matthew Bender, Revised Edition) (retailers who accept checks purchase DMV records in bulk to verify the personal information of consumers using checks).

5. Defendant's practice is to ask for the Driver's License of a customer wishing to buy certain items and, once the customer's driving record is in Defendant's possession, without notice or consent, to scan that license's barcode. If Defendant already has a copy of this information in its database, the customer's purchase information is simply associated with the customer's existing motor vehicle record. If Defendant does not have a copy of this information, Defendant captures all the personal information on the customer's Drivers License, effectively creating a new motor vehicle record in its database. This new record is then associated with the customer's purchase information. *See* Duhigg *supra* ("If you use a credit card or a coupon, or fill out a survey, or mail in a refund, or call the customer help line, or open an e-mail we've sent you

or visit our Web site, we'll record it and link it to your Guest ID."). All of this occurs either in real-time at the time of purchase or is resolved at some later time by Defendant's technicians, programmers, or data scientists who maintain and analyze the data stored in Defendant's data warehouse. *See* http://www.teradata.com/News-Releases/2012/Teradata-Selected-by-Target-Corporation-as-Database-Analytics-Partner/ (*accessed on* Feb. 5, 2016 at 3:54 PM).

6. While stating that the consumer's Drivers License is necessary for verification of some type, Defendant instead takes **all** information from the Drivers License and **keeps** this information as part of its consumer database.

7. Defendant by its own admission keeps and maintains a customer database of all information obtained from driving records, and by its own admission uses that information in contravention of various state and federal privacy laws [including but not limited to the Driver's Privacy Protection Act, 18 U.S.C. § 2721 *et seq*.] to, *inter alia*, sell and republish that personal information to third parties and to track Defendant sales and purchase histories of customers.

8. Defendant has taken no step to obtain express verbal or written permission to collect sensitive and personal information from Customers' driving records as required by statute, and indeed it has no such permission from its Customers.

9. Defendant does not attempt to inform Customers that information obtained from their driving records was being collected, tracked, stored and republished in its customer databases.

Plaintiff Stephen Nick

10. Plaintiff Stephen Nick is a resident of Suffolk County, New York and is a customer of Defendant.

11. Plaintiff Nick attempted to buy and did buy over-the-counter medicine from

Defendant at the Target store at Suffolk County, New York on multiple occasions within the last three years, with the latest occurrence on June 23, 2015.

12. When paying for the over-the-counter medicine at Defendant's cash register, Plaintiff Nick was consistently asked for and did surrender his Driver's License to Defendant's employee. The employee captured all of the information from Plaintiff Nick's Driver's License with an optical scanning device.

13. The scanning of Plaintiff Nick's Driver's License caused Plaintiff Nick's purchase information to be associated with an existing motor vehicle record that Defendant had purchased from the department of motor vehicles.

14. Defendant collected and used this newly acquired information in conjunction with Plaintiff Nick's existing motor vehicle records for marketing purposes.

15. Defendant knew or should have known that Plaintiff Nick never expressly consented to the release of his DMV records for marketing or solicitation purposes.

16. Defendant did not obtain or even attempt to obtain Plaintiff Nick's express consent to use his DMV records for marketing or solicitation purposes.

17. On June 23, 2015, Plaintiff Nick asked Defendant's employee why his Drivers License was swiped and was told federal law required it for the sale of pseudoephedrine.

18. Defendant could have sold Plaintiff Nick his over-the-counter medicine without swiping his Drivers License.

19. If Plaintiff Nick knew he could still make his purchases and refuse to hand over his Drivers License, he would not have handed over his Drivers License to Defendant.

20. If Plaintiff Nick knew that Defendant would collect and keep PII from his Drivers License, he would not have make his purchases from Defendant.

21. Plaintiff Nick was never informed his Driver's License would be optically read and **all** the information from it retained by Defendant.

22. Plaintiff Nick never consented to allow Defendant to collect the information from his Driver's License or agreed to have that personal information retained by Defendant for any purpose.

23. Plaintiff Nick was never given an opportunity to opt out of this furtive assembling of personal information from his driver's license.

24. Defendant's employee never asked verbal or written permission to collect that Driver's License information, nor did it receive any such permission or consent.

25. Plaintiff Nick intends to continue to purchase over-the-counter medicine from Defendant.

Plaintiff Matthew Dash

26. Plaintiff Matthew Dash is a resident of Nassau County, New York and is a customer of Defendant.

27. Plaintiff Dash is over 40 years old.

28. Plaintiff Dash attempted to buy and did buy a video game from Defendant at the Target store at 999 Corporate Drive, Westbury, Nassau County, New York in December 2012.

29. When paying for the game at Defendant's cash register, without reason, Plaintiff Dash was asked for and did surrender his Driver's License to Defendant's employee. The employee captured all of the information from Plaintiff Dash's Driver's License with an optical scanning device.

30. The scanning of Plaintiff Dash's Driver's License caused Plaintiff Dash's purchase information to be associated with an existing motor vehicle record that Defendant had

purchased from the department of motor vehicles.

31. Defendant collected and used this newly acquired information in conjunction with Plaintiff Dash's existing motor vehicle records for marketing or solicitation purposes.

32. Defendant knew or should have known that Plaintiff Dash never expressly consented to the release of his DMV records for marketing or solicitation purposes.

33. Defendant did not obtain or even attempt to obtain Plaintiff Dash's express consent to use his DMV records for marketing or solicitation purposes.

34. There is no basis in law for Defendant to require age verification for Plaintiff Dash's purchase.

35. Plaintiff Dash did not know he could refuse to hand over his Drivers License and still make his purchase.

36. Plaintiff Dash was never informed his Driver's License would be optically read and all the information from it retained by Defendant.

37. Plaintiff Dash never consented to allow Defendant to collect the information from his Driver's License much less agree to have that personal information retained by Defendant for any purpose.

38. Plaintiff Dash was never given an opportunity to opt out of this furtive assembling of personal information from his driver's license.

39. Defendant could have sold Plaintiff Dash his game without Plaintiff Dash handing over his Drivers License.

40. If Plaintiff Dash knew he could make his purchase and refuse to hand over his Drivers License, he would not have handed over his Drivers License to Defendant.

41. If Plaintiff Dash knew that Defendant would collect and keep PII from his Drivers

License, he would not have make his purchase from Defendant.

42. Defendant's employee never asked verbal or written permission to collect that Driver's License information, nor did it receive any such permission or consent.

43. Defendant's Driver's License scanning and data retention policy are not written on the transaction receipt nor posted at the register, nor posted anywhere in the store.

44. Plaintiff Dash intends to continue to purchase age-verified games and other products from Defendant.

Defendant

45. Defendant Target Corporation ["Target"] is a Minnesota corporation with its headquarters at 1000 Nicollet Mall, Minneapolis, Minnesota. Its common stock is listed on the New York Stock Exchange under the symbol "TGT."

46. Defendant operates general merchandise stores in the US employing over 350,000 full-time, part-time and seasonal employees.

47. Target filed its latest Form 10-Q Quarterly Financials with the SEC on November 21, 2014 [the "Nov. 2014 10-Q"] to report on the quarterly period ended November 1, 2014.

48. Target reported sales in the United States for the nine months ended November 1, 2014 as $50,868,000,000.00 from 1,801 stores in the United States.

49. In the Nov. 2014 10-Q, Target states: "An important component of our business involves the receipt and storage of information about our guests and team members."

50. In its Form 10-Q Quarterly Financials filed with the SEC November 21, 2012 [the "Nov. 2012 10-Q"], Target lists as an asset "Company Guest Data"

51. It defines the term in its Nov. 2012 10-Q as:

> "Company Guest Data" means all personally identifiable information regarding a Company Guest that is obtained by Company (other than solely

> in its capacity as servicer) in connection with the Company Guest making a purchase of Goods and/or Services, including all transaction, experience and purchase information collected by Company (other than in its capacity as servicer) with regard to each purchase of Goods and/or Services made by a Company Guest, including the item-specific transaction information collected about Cardholders in connection with any such purchase of Goods and/or Services.

52. Defendant admits in the media and its SEC filings to collecting said data and admits to the illegal collection of Driver's License records; done knowingly and in the normal course of business for Defendant.

53. Defendant admits in the media and its SEC filings to the illegal use of the wrongfully collected Driver's License data.

VENUE AND JURISDICTION

54. Venue in this Court is proper because many of Defendant's retail stores are located in this Judicial District and because a substantial part of the acts or omissions giving rise to the claims in this action occurred in this Judicial District.

55. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d), because (a) the class has more than 100 members, (b) at least one of the members of the proposed class is a citizen of a state other than New York, and (c) the total amount in controversy exceeds $5 million exclusive of interest and costs.

56. This Court has personal jurisdiction over Defendant because a substantial portion of the wrongdoing alleged in this Complaint took place in this District, Defendant is authorized to do business in this District, Defendant has sufficient minimum contacts with this District through, *inter alia*, the operation of retail stores, and/or otherwise intentionally avails itself of the markets in this District through the promotion, marketing, and sales in this District so that the

exercise of personal jurisdiction of this Court complies with judicial notions of fair play and substantial justice.

GENERAL ALLEGATIONS

The Illegal Scanning of Driver's Licenses by Defendant

57. Target maintains and operates approximately 1,801 retail stores in the United States. In its general retail operations, it employs computerized "point of sale" ["POS"] computer terminals at each of its cash registers.

58. Each of these terminals is connected to a main computer system within the store, which is in turn connected to Defendant's corporate computer network.

59. Defendant carefully tracks and maintains records of the buying habits of customers, calling those customers "Company Guests"

60. From the Nov. 2012 10-Q: "'Company Guests' means any Person who makes purchases of Goods and/or Services."

61. Timing is everything in retail, as Defendant states in its Annual Report 10-K for 2011 filed March 11, 2011 ["2011 10-K"] with the SEC:

> Effective inventory management is key to our ongoing success. We utilize various techniques including demand forecasting and planning and various forms of replenishment management. We achieve effective inventory management by being in-stock in core product offerings, maintaining positive vendor relationships, and carefully planning inventory levels for seasonal and apparel items to minimize markdowns.

62. Target also states in its 2011 10-K: "We rely extensively on our computer systems to manage inventory, process guest transactions and summarize results."

63. Target also states in its 2011 10-K: "The nature of our business involves the receipt and storage of personal information about our guests."

64. On the company's website, a page titled "Privacy Policy" at URL

http://www.target.com/spot/privacy-policy#InfoCollected Defendant states its collection of data occurs, *inter alia*, at its retail store registers:

> *What Information is Collected?*
> We collect information from the following:
> Information you give us when interacting with Target, for example, in stores […]

65. That same web page spells out what type of data is collected by Defendant:

> Types of information we collect include:
> **Your name**
> **Your mailing address**
> Your e-mail address
> **Your phone (or mobile) number**
> **Your drivers' license number**

(Emphasis added). As stated *supra*, the Act lists these items as "personal information" not to be collected from a motor vehicle record.

Age Verification and Pseudoephedrine Purchase Legal Verification Requirements

66. In purchasing certain items, Defendant requires a customer to hand over their Drivers License for "verification" of age or the like, and instead of simply verifying the information by eye, as would be expected, swipes the driver's record and captures the PII from it (hereinafter a "Swipe" or "Swiping").

67. Defendant does not ask permission to Swipe customers' Drivers Licenses.

68. Defendant's Swiping of Plaintiffs' Drivers Licenses and capture of the PII therefrom cannot be justified as an anti-fraud measure.

69. There was no disclosure at the Point of Sale that Defendant would Swipe Plaintiffs' Drivers Licenses and captures the PII therefrom.

70. Certainly, Defendant did not get written consent from Plaintiffs or any customer to capture and retain the PII from their Drivers Licenses.

71. Defendant does not post notice to the public of its policy to capture the PII from its customers' Drivers Licenses when Defendant requests them for "verification."

72. Defendant does not post notice to the public of its policy to capture the PII from its customers' Drivers Licenses when it displays its refund policy as to all goods as required by law.

73. There is no sign posted at each store entrance used by the public in Defendant's stores that provides notice to the public of its policy to capture the PII from its customers' Drivers Licenses.

74. Similarly, there is no verbiage on the sales receipt, verbiage attached to an item for sale, or sign affixed to each cash register or point of sale alerting the public of Defendant's policy to capture the PII from its customers' Drivers Licenses.

75. Defendant has not posted notice of its Driver's License scanning and data retention policy anywhere in its stores.

76. Defendant never seeks nor is granted the express, written consent necessary to obtain personal information from a Driver's License issued by a state division of motor vehicles.

77. Defendant does not obtain the consent of customers when it collects Driver's License information, either verbal or written: there is no opt-in or opt-out procedure to this surreptitious and illegal data gathering.

78. There are valid reasons Defendant may ask for a Driver's License but none involves capture and dissemination of personal Driver's License information. Confirming age of an individual is one of these and Defendant states this on its website.

> Conduct a transaction where we collect information required by law (for example, pseudoephedrine or age-restricted purchases)

79. Collection (much less retention) of Driver's License information is not necessary

to carry out the implied or stated goal of age verification.

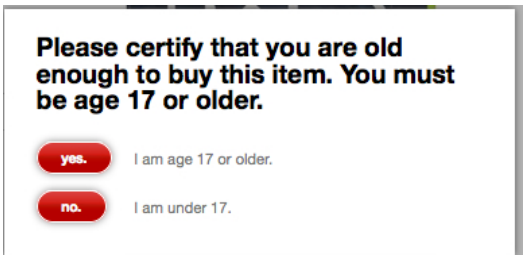
80. In reality, Defendant does not really Swipe Driver's License information as a prerequisite of an age restricted purchase.

81. If a patron makes enough of a scene and asks to speak with management, on occasion this "inviolate" company policy of age verification through Driver's License Swipes will be waived.

82. The "age-restricted purchase" Plaintiff Dash made from Defendant was a video game rated "M" by the Entertainment Software Rating Board ("ESRB") which on its website describes itself as "the non-profit, self-regulatory body that assigns ratings for video games and apps so parents can make informed choices. The ESRB rating system encompasses guidance about age-appropriateness, content, and interactive elements."[1]

83. An "M" designation is described by the ESRB as "MATURE - Content is generally suitable for ages 17 and up. May contain intense violence, blood and gore, sexual content and/or strong language." There is no current state law that requires a game to carry ANY rating or a vendor to verify age of purchaser for games rated "M."

84. In fact, if you were to try to buy the same game Plaintiff purchased in the store from Defendant's website, the age verification process is a pop-up window that asks:



85. Were you to answer "yes" the game is added to your cart. No account needs to be

[1] http://www.esrb.org/ratings/ratings_guide.jsp

established to buy the item, and you can pay with Target GiftCard or PayPal, neither of which verifies age.

86. In the purchase of pseudoephedrine and other similar over-the-counter medicines, Defendant has a legal recording requirement to track the names and addresses of purchasers and the amount of the over-the-counter medicine purchased.

87. In selling over-the-counter medicines, Defendant swipes a purchaser's Drivers License, capturing much more information than is necessary to comply with laws regarding the recording of over-the-counter medicine sales.

88. For example, purchase of over-the-counter medicine containing ephedrine, pseudoephedrine, or phenylpropanolamine (hereinafter "Listed OTCs") is subject to the "Combat Methamphetamine Epidemic Act of 2005" (hereinafter the "CME Act").

89. The CME Act amends the Controlled Substances Act (21 U.S.C. 801 *et sec.*) (hereinafter the "CSA") with regard to record keeping on the purchase of the Listed OTC medications.

90. With the 2005 federal CME Act, the sellers of Listed OTCs are required to keep a logbook with the names, addresses, and signatures of purchasers.

91. CSA Section 830 (e)(1)(A)(iii) requires a "seller maintain a written or electronic list of such sales that identifies the products by name, the quantity sold, the names and addresses of purchasers, and the dates and times of the sales (which list is referred to in this subsection as the 'logbook')."

92. For each purchase, CSA Section 830 (e)(1)(A)(iv)(I)(aa) requires a purchaser present "an identification card that provides a photograph and is issued by a State or the Federal Government"

93. CSA Section 830 (e)(1)(A)(iv)(I)(bb) requires a purchaser to "sign[] the written logbook and enters in the logbook his or her name, address, and the date and time of the sale."

94. If the seller uses an electronic logbook, CSA Section 830 (e)(1)(A)(iv)(I)(bb)(AA)-(CC) dictate the acceptable methods a purchaser signature may be recorded: "[s]igning a device presented by the seller that captures signatures in an electronic format;" "[s]igning a bound paper book;" or "[s]igning a printed document that includes, for such purchaser, the name of each product sold, the quantity sold, the name and address of the purchaser, and the date and time of the sale."

95. CSA Section 830 (e)(1)(A)(iv)(III) requires the information in the "logbook maintained by the seller includes the prospective purchaser's name, address, and the date and time of the sale, as follows:

> (aa) If the purchaser enters the information, the seller must determine that the name entered in the logbook corresponds to the name provided on such identification and that the date and time entered are correct.
> (bb) If the seller enters the information, the prospective purchaser must verify that the information is correct.
> (cc) Such information may be captured through electronic means, including through electronic data capture through bar code reader or similar technology.

96. Defendant's policy of requesting a customer to hand over their Drivers License for "verification" of consumer transactions not involving the Controlled Substances Act and instead Swiping for capture of PII for its customer database is a deceptive practice under General Business Law § 349 and the analogous state DPA's.

Data Collection and Warehousing

97. The true reason Defendant bends over backwards to collect Driver's License information is simple and clear: data is valuable.

98. Defendant retains the secretly obtained Driver's License information and

republishes it to various parties.

99. Again, from the Defendant's website page titled "Privacy Policy":

> *Sharing with Other Companies (for their marketing purposes)*
> We may share information with vendors, business partners and other organizations [*sic*] which are not part of the Target family. These companies and organizations may use the information we share to provide special offers and opportunities to you.

100. Defendant considers this ill-gotten Driver's License information so valuable they disclose it as a valuable business asset in their SEC filings.

101. In a former iteration of its website page titled "Privacy Policy," Defendant stated:

> *Business Transfers*
> If some or all of our business assets are sold or transferred, we generally would transfer the corresponding information regarding our guests. We also may retain a copy of that guest information.

102. Currently, that section reads, "If some or all of our business assets are sold or transferred, we **may** transfer the corresponding information regarding our guests. We also may retain a copy of that guest information" (emphasis added).

103. Such a transfer will occur with Defendant's sale of 1,600 drugstores to CVS.

104. In a New York Times article on June 15, 2015, titled "CVS to Buy 1,600 Drugstores From Target for $1.9 Billion," CVS will "acquire more than 1,600 pharmacies from Target in 47 states and operate them under the CVS name in Target stores."[2]

105. This is a longstanding business practice for Defendant. The website "Privacy Policy" page lists all "Target Privacy Policy Revisions" since 2004. It states the "Last update: 07/31/2014" and in the list of revisions does not discuss Driver's License information, although the Driver's Privacy Protection Act has been federal law since 1994.

[2] http://www.nytimes.com/2015/06/16/business/dealbook/cvs-agrees-to-buy-targets-pharmacy-business-for-1-9-billion.html?_r=0

106. Consumer histories that can be tied together to show more than one transaction are called "customer-level datasets." They are extremely valuable and jealously guarded.

107. Consumer data of someone that drives a car is even more valuable to Defendant, as that person probably has assets (a car, for example) and an existing "data footprint" enabling a retailer to cobble together purchase histories and the like.

108. With the merger of CVS and Target, all consumer data collected by Defendant will no be tied to even more medical information and history.

109. Consumers' individual buying histories are crucial in behavioral targeting, personalization of branding, targeted marketing, and market segmentation strategies.

110. Accenture is self described as "a global management consulting, technology services and outsourcing company, with 257,000 people serving clients in more than 120 countries". This high powered think-tank drives home the value of "big-data" in its publication Outlook:

> While other competitive "essentials" fall in and out of fashion, growth remains the defining measure of business success—it's how markets assess companies and leaders gauge their performance against peers. But achieving adequate growth in today's often-difficult competitive environment means everyone and everything in an organization needs to work harder than ever. Companies endowed with massive amounts of customer information can use it to supercharge their growth engines, potentially making Big Data a very big deal indeed.

111. Clearly, these areas are no trivial matter to business people. Wharton School of the University of Pennsylvania offers to its MBA program "The Wharton Customer Analytics Initiative." They describe the discipline of customer analytics:

> Many businesses have come to the recent realization that customer analytics is at the heart of what will give them a competitive edge, yet they are often stymied by their inability to pursue sophisticated modeling tasks to address critical strategic questions. Responding to this need, the WCAI helps companies leverage their customer-level datasets by serving as a "matchmaker" between these firms and

> top scholars from multiple disciplines (e.g. marketing, information systems, computer science, operations research) around the world.

112. Given the potential huge profits from the tracking of consumer information, companies are willing to spend huge sums of money for the software to make sense of the data sets. International Data Corporation ("IDC"), a leading market research firm for technology, estimates the market for business analytics software grew 14 percent in 2011 and will hit $50.7 billion in revenue by 2016.[3]

113. The development of proprietary data sets can have a huge influence on the success of marketing and retailing projects.

114. It is no wonder that retailers are willing to fly in the face of reason to collect consumer data to tie to buying histories and transactions. In a piece titled "Multiple retailers start requiring a driver's license swipe,"[4] abc7news.com in California noted a couple's concern:

> No one would doubt that Carolyn and Gene Taylor are old enough to drink; after all, she's 64 and he's 75. So it was a complete shock when they tried to buy liquor at a Rite Aid store in Oakley.
> "The clerk asked me to take my driver's license out of my wallet and to scan it. I said 'Why?'" said Carolyn. "It was just to prove you were old enough to buy alcohol."
> "We thought it was rather strange, seeing I'm almost 76 years old and getting carded. That is kind of different," said Gene.
> Carolyn swiped her license anyway, went to her car with her two bottles, and then suddenly had a terrible thought.
> "It's out there. The cat's out of the bag now that I consume alcohol," said Carolyn. "I thought, 'Great, now what have I done?' I thought, 'I bet my health insurance is going to go up,' or 'Is my car insurance going to go up?'"

115. The retention and republication of Driver's License personal information as in the case of the Taylors also violates California state law:

> Cal. Civil Code: CONFIDENTIALITY OF DRIVER'S LICENSE

[3] http://www.businesswire.com/news/home/20120711005235/en/Worldwide-Business-Analytics-Software-Market-Continues-Stellar#.VZ6AGxNViko
[4] http://abc7news.com/archive/7441118/

> INFORMATION
> 1798.90.1. (a) (1) Any business may swipe a driver's license or identification card issued by the Department of Motor Vehicles in any electronic device for the following purposes:
>
> (A) To verify age or the authenticity of the driver's license or identification card.
>
> (B) To comply with a legal requirement to record, retain, or transmit that information.
>
> (C) To transmit information to a check service company for the purpose of approving negotiable instruments, electronic funds transfers, or similar methods of payments, provided that only the name and identification number from the license or the card may be used or retained by the check service company.
>
> (D) To collect or disclose personal information that is required for reporting, investigating, or preventing fraud, abuse, or material misrepresentation.
>
> (2) A business may not retain or use any of the information obtained by that electronic means for any purpose other than as provided herein.
>
> (b) As used in this section, "business" means a proprietorship, partnership, corporation, or any other form of commercial enterprise.
>
> (c) A violation of this section constitutes a misdemeanor punishable by imprisonment in a county jail for no more than one year, or by a fine of no more than ten thousand dollars ($10,000), or by both.

116. In a piece titled "Target Requires Driver's License Scan For Restricted Items" the author states "Target called to assure me that only date-of-birth information is captured from the magnetic strip." As demonstrated *infra*, Target obtains, retains discloses and republishes more than just your date of birth. The author continues, "I don't think so. I mean, really, I have an easier time buying liqueur at the state store than nicotine-laced gum at Target."[5]

What Data Is Contained In a Driver's License Barcode?

117. Information technology allows data to be stored in a graphic format commonly called a barcode. The International Organization for Standardization ("ISO") has a definition of

[5] http://www.darkreading.com/risk-management/target-requires-drivers-license-scan-for-restricted-items/d/d-id/1081246?

the standard[6]:

> The technology of bar coding is based on the recognition of patterns of bars and spaces of defined dimensions. There are various methods of encoding information in bar code form, known as symbologies, and the rules defining the translation of characters into bars and space patterns and other essential features are known as the symbology specification.

118. The ISO currently publishes ISO/IEC 18013-2:2008 Information technology -- Personal identification -- ISO-compliant driving license -- Part 2: Machine-readable technologies. The ISO summary of the "ISO-compliant driving license" elements:

> Mandatory and optional machine-readable data. Machine-readable IDL data support the following functions (subject in some cases to the inclusion of appropriate optional data elements):
> confirming the driving privileges of a driver;
> enabling a link to be established to a driving privilege database;
> age verification;
> identity verification;
> biographical data verification;
> evidence of residence;
> biometric authentication;
> document authentication and validation.

119. On the back of every state issued Driver's License is a machine readable barcode containing personal information as defined in the Driver's Privacy Protection Act.

120. PDF417 is the standard symbology specification selected by the Department of Homeland Security as the barcode technology for RealID compliant driver licenses and state issued identification cards.

121. On the Honeywell corporate website[7], this definition of PDF417 is informative:

> PDF417 is a 2-dimensional stacked barcode created by Symbol Technologies in 1991. It is one of the most popular 2D codes because of its ability to be read with slightly modified handheld laser or linear CCD scanners. PDF stands for Portable Data File and 417 represents the 17 modules of 4 bars and spaces that make up

[6] http://www.iso.org/iso/catalogue_detail.htm?csnumber=43897
[7] http://www.omniplanar.com/PDF417-2D-Barcode.php

each code.

122. Physical specifications of the PDF417 standard are detailed in ISO/IEC 15438:2006(E) Information technology — Automatic identification and data capture techniques — PDF417 bar code symbology specification.

123. The American Association of Motor Vehicle Administrators (aamva.org) publishes the standards that the individual states follow when designing their driver's licenses in its document titled ANSI-D20 2009 - Standard for Traffic Records Systems.[8] ANSI-D20 on pages 199 to 205 lists mandatory and optional data elements (called "person elements") about a driver on a Driver's License barcode including driver name, address, date of birth, height, weight, eye and hair color, race or ethnicity, sex, social security number, military service history, and driver "points" for driving infractions. "Driver's License elements" contained in a Driver's License barcode include a commercial classification code, endorsement code, "driver license expiration date", Driver's License number and issuance date. Within the barcode is also the driver's Organ Donor status.

124. On the State of New York Department of Motor Vehicles website is a letter from then Commissioner David J. Swarts confirming "PDF 417 2D barcode will be printed on the back of both standard and enhanced licenses.[9] The barcode content will conform to the current AAMVA specification: DL/ID Card Design Specification Ver 2.0 March 2005. The length of the barcode will be increased to 325 bytes."

125. The letter confirms that the Driver's License number as well as personal information as defined in the Driver's Privacy Protection Act is contained in the barcode of New York drivers, including that of Plaintiffs.

[8] http://www.aamva.org/ANSI-D20-Standard-for-Traffic-Records-Systems/
[9] http://dmv.ny.gov/ii-es/7-8-08changesnyslicenseandndid.pdf

Driver's Privacy Protection Act

126. Congress enacted a law to protect the personal information contained on a Driver's License and other motor vehicle records without the driver's written consent. The statute is 18 U.S.C. §2721 *et seq*., titled the Driver's Privacy Protection Act (the "Act" or the "DPPA").

127. 18 U.S.C. § 2722 makes it "unlawful for any person knowingly to obtain or disclose personal information, from a motor vehicle record, for any use not permitted under section 2721(b) of this title."

128. "Personal information" is defined in 18 U.S.C. § 2725(3) including "personal information" defined as "information that identifies an individual, including an individual's photograph, social security number, **driver identification number, name, address** (but not the 5-digit zip code), **telephone number**…" and "highly restricted personal information" is defined in 18 U.S.C. § 2725(4).

129. 18 U.S.C. §2721 is titled "Prohibition on release and use of certain personal information from State motor vehicle records" and subsection (b) limits the permissible uses of personal information obtained from a motor vehicle record "by a business" **only** to verify information submitted by the individual to the business **or** "or the purposes of preventing fraud by, pursuing legal remedies against, or recovering on a debt or security interest against, the individual."

130. 18 U.S.C. § 2724(a) makes it illegal to knowingly obtain, disclose or use personal information, from a motor vehicle record for a purpose not permitted under the DPPA and allows a federal civil action against such violation, stating that an individual can bring a civil action against a "person who knowingly obtains, discloses or uses personal information, from a motor

vehicle record, for a purpose not permitted under this chapter ... for liquidated damages in the amount of $2,500 ... punitive damages ... reasonable attorneys' fees and other litigation costs ... and ... preliminary and equitable relief....”

131. Defendant knowingly and intentionally obtained Plaintiffs’ personal information and highly restricted personal information from a motor vehicle record when scanning Plaintiffs’ Drivers’ License without their knowledge or consent.

132. Defendant’s knowing and intentional acquisition of Plaintiffs’ personal information or highly restricted personal information is not a “use in the normal course of business” as described by the Act.

133. Defendant’s knowing and intentional acquisition of Plaintiffs’ personal information or highly restricted personal information is deceptive in that Defendant avers its actions are legal or required by law.

134. Defendant’s policy of requesting a customer to hand over their Drivers License for “verification” of consumer transactions not involving the Controlled Substances Act and instead Swiping for capture of PII for its customer database is a deceptive practice under General Business Law § 349 and the analogous state Deceptive Practice Acts or consumer protection laws (“DPAs”).

135. Defendant’s policy of requesting a customer to hand over their Drivers License for “verification” of consumer transactions involving the Controlled Substances Act and instead Swiping for capture of more PII than required under CSA Section 830 (e)(1)(A)(iv)(III) for use in its customer database is a deceptive practice under General Business Law § 349 and the analogous state DPAs.

136. Defendant's conduct is also a violation of the 18 U.S. Code § 2722(b), which makes it unlawful to make a false representation to obtain any personal information from an individual's motor vehicle record.

137. Plaintiffs and the Class they seek to represent may bring civil action against Defendant for this conduct under DPPA § 2724 for damages and attorneys' fees.

FIRST CAUSE OF ACTION
Violation of the Driver's Privacy Protection Act

138. Plaintiffs repeat and reallege the allegations of Paragraphs 1-125 with the same force and effect as though fully set forth herein.

139. Defendant obtained personal information from Plaintiffs and Class Members' driver's licenses without the requisite consent of Plaintiffs and Class Members under 18 U.S.C. § 2721 *et seq.*

140. 18 U.S.C. § 2722(b) states that it is "unlawful for any person to make false representation to obtain any personal information from an individual's motor vehicle record."

141. 18 U.S.C. § 2725(3) defines "personal information" as "information that identifies an individual, including an individual's photograph, social security number, driver identification number, name, address (but not the 5-digit zip code), telephone number, and medical or disability information, but does not include information on vehicular accidents, driving violations, and driver's status."

142. 18 U.S.C. § 2725(4) defines "highly restricted personal information" as "an individual's photograph or image, social security number, medical or disability information."

143. Defendant wrongfully takes and retains personal information and highly restricted personal information from its customers' Drivers Licenses in the normal course of its business under the false representation of age verification.

144. Defendant wrongfully takes and retains personal information and highly restricted personal information from its customers' Drivers Licenses in the normal course of its business under the false representation of control of over-the-counter medications.

145. 18 U.S.C. § 2724 provides that an individual can bring a civil action against a "person who knowingly obtains, discloses or uses personal information, from a motor vehicle record, for a purpose not permitted under this chapter ... for liquidated damages in the amount of $2,500 ... punitive damages ... reasonable attorneys' fees and other litigation costs ... and ... preliminary and equitable relief...."

146. Defendant knowingly obtained Plaintiffs' and Class Members' personal information or highly restricted personal information from motor vehicle records when it scanned Plaintiffs' and Class Members' driver's licenses without consent and for an impermissible purpose.

147. Defendant's knowing acquisition of Plaintiffs and Class Members' personal information or highly restricted personal information is not a "use in the normal course of business" as described by the Act.

148. Defendant admits as detailed *infra* that it knowingly uses this captured personal information or highly restricted personal information without consent.

149. As the result of Defendant's conduct, Plaintiffs and the Class were harmed.

SECOND CAUSE OF ACTION
Breach of GBL 349
(On Behalf of Plaintiffs and the New York Subclass)

150. Plaintiffs repeat and reallege the allegations of Paragraphs 1-125 with the same force and effect as though fully set forth herein.

151. Defendant obtains, discloses, or uses personal information from a motor vehicle record without knowledge or consent of Plaintiffs and the Class as described herein, which

constitutes the "conduct of any trade or commerce" within the meaning of NYS GBL § 349.

152. Defendant, in the normal course of their business, collected user information implying or stating that such data would be used for the legitimate purpose of age or other verification.

153. Defendant misrepresents the collection, storage, amount, and use of personal information from Driver's License it wrongfully obtains.

154. In the collection and use of this personal information from a state issued Driver's License without a legitimate or lawful purpose, Defendant violates consumer protection statutes and/or state deceptive business practices statutes.

155. Further, by violating 18 U.S.C. § 2722(b), Defendant engaged in a deceptive consumer practice in its normal course of business.

156. By Defendant's deceptive actions, Plaintiffs and the Class were harmed.

THIRD CAUSE OF ACTION
Fraudulent Concealment/Nondisclosure
(On Behalf of Plaintiffs and the Nationwide Class)

157. Plaintiffs repeat and reallege the allegations of Paragraphs 1-125 with the same force and effect as though fully set forth herein.

158. Defendant actively concealed from and failed to disclose to Plaintiffs and the Class the true nature of the collection, storage, and use of PII from driver's licenses it wrongfully obtains as described above.

159. Defendant was under a duty to Plaintiffs and the Class to disclose these facts under the DPPA and by good faith, fair dealing, and yet Defendant actively concealed the real purpose of its acts.

160. This fact concealed by Defendant from Plaintiffs and the Class is a material fact

in that Defendant has a legal obligation to disclose its collection of personal information from a driver's license.

161. Defendant intentionally concealed and failed to disclose the true facts about the collection for the purpose of inducing Plaintiffs and the Class to hand over their driver's licenses.

162. Had Plaintiffs and the Class known of the surreptitious collection of their personal information, they would not have allowed it to occur.

163. As the result of Defendant's conduct, Plaintiffs and the Class were harmed.

FOURTH CAUSE OF ACTION
Violation of the Consumer Fraud and Deceptive Trade Practices Acts
of the Various States and District of Columbia
(On Behalf of the non-New York Class)

164. Plaintiffs repeat and reallege the allegations of Paragraphs 1-125 with the same force and effect as though fully set forth herein.

165. By violating 18 U.S.C. § 2722(b), Defendant engaged in a deceptive consumer practice in its normal course of business.

166. By Defendant's deceptive actions, Plaintiffs and the class were harmed.

167. Plaintiffs bring this Count individually, and on behalf of all similarly situated residents of each of the other states and the District of Columbia for violations of the respective statutory DPAs and consumer protection laws, as follow:

A. the Alabama Deceptive Trade Practices Act, Ala.Code 1975, § 8–19–1, *et seq*.;

B. the Alaska Unfair Trade Practices and Consumer Protection Act, AS § 45.50.471, *et seq*.;

C. the Arizona Consumer Fraud Act, A.R.S §§ 44-1521, *et seq*.;

D. the Arkansas Deceptive Trade Practices Act, Ark.Code §§ 4-88-101, *et seq*.;

E. the California Unfair Competition Law, Bus. & Prof. Code §§17200, *et seq*. and 17500 *et seq*.;

F. the California Consumers Legal Remedies Act, Civil Code §1750, *et seq*.;

G. the Colorado Consumer Protection Act, C.R.S.A. §6-1-101, *et seq*.;

H. the Connecticut Unfair Trade Practices Act, C.G.S.A. § 42-110, *et seq*.;

I. the Delaware Consumer Fraud Act, 6 Del. C. § 2513, *et seq*.;

J. the D.C. Consumer Protection Procedures Act, DC Code § 28-3901, *et seq*.;

K. the Florida Deceptive and Unfair Trade Practices Act, FSA § 501.201, *et seq*.;

L. the Georgia Fair Business Practices Act, OCGA § 10-1-390, *et seq*.;

M. the Hawaii Unfair Competition Law, H.R.S. § 480-1, *et seq*.;

N. the Idaho Consumer Protection Act, I.C. § 48-601, *et seq*.;

O. the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 501/1 *et seq*.;

P. the Indiana Deceptive Consumer Sales Act, IN ST § 24-5-0.5-2, *et seq*.;

Q. the Iowa Private Right of Action for Consumer Frauds Act, Iowa Code Ann. § 714H.1, *et seq*.;

R. the Kansas Consumer Protection Act, K.S.A. § 50-623, *et seq*.;

S. the Kentucky Consumer Protection Act, KRS 367.110, *et seq*.;

T. the Louisiana Unfair Trade Practices and Consumer Protection Law, LSA-R.S. 51:1401, *et seq*.;

U. the Maine Unfair Trade Practices Act, 5 M.R.S.A. § 205-A, *et seq*.;

V. the Maryland Consumer Protection Act, MD Code, Commercial Law, § 13-301, *et seq*.;

W. the Massachusetts Regulation of Business Practices for Consumers Protection Act, M.G.L.A. 93A, *et seq*.;

X. the Michigan Consumer Protection Act, M.C.L.A. 445.901, *et seq*.;

Y. the Minnesota Prevention of Consumer Fraud Act, Minn. Stat. § 325F.68,

et seq.;

Z. the Mississippi Consumer Protection Act, Miss. Code Ann. § 75-24-1, *et seq*.;

AA. the Missouri Merchandising Practices Act, V.A.M.S. § 407, *et seq*.;

BB. the Montana Unfair Trade Practices and Consumer Protection Act of 1973, Mont. Code Ann. § 30-14-101, *et seq*.;

CC. the Nebraska Consumer Protection Act, Neb.Rev.St. §§ 59-1601, *et seq*.;

DD. the Nevada Deceptive Trade Practices Act, N.R.S. 41.600, *et seq*.;

EE. the New Hampshire Regulation of Business Practices for Consumer Protection, N.H.Rev.Stat. § 358-A:1, *et seq*.;

FF. the New Jersey Consumer Fraud Act, N.J.S.A. 56:8, *et seq*.;

GG. the New Mexico Unfair Practices Act, N.M.S.A. §§ 57-12-1, *et seq*.;

HH. the North Carolina Unfair and Deceptive Trade Practices Act, N.C. Gen Stat. § 75-1.1, *et seq*.;

II. the North Dakota Consumer Fraud Act, N.D. Cent.Code Chapter 51-15, *et seq*.;

JJ. the Ohio Consumer Sales Practices Act, R.C. 1345.01, *et seq*.;

KK. the Oklahoma Consumer Protection Act, 15 O.S.2001, §§ 751, *et seq*.;

LL. the Oregon Unlawful Trade Practices Act, ORS 646.605, *et seq*.;

MM. the Pennsylvania Unfair Trade Practices and Consumer Protection Law, 73 P.S. § 201-1, *et seq*.;

NN. the Rhode Island Deceptive Trade Practices Act, G.L.1956 § 6-13.1-5.2(B), *et seq*.;

OO. the South Carolina Unfair Trade Practices Act, SC Code 1976, §§ 39-5-10, *et seq*.;

PP. the South Dakota Deceptive Trade Practices and Consumer Protection Act, SDCL § 37-24-1, *et seq*.;

QQ. the Tennessee Consumer Protection Act, T.C.A. § 47-18-101, *et seq*.;

RR. the Texas Deceptive Trade Practices-Consumer Protection Act, V.T.C.A., Bus. & C. § 17.41, *et seq*.;

SS. the Utah Consumer Sales Practices Act, UT ST § 13-11-1, *et seq*.;

TT. the Vermont Consumer Fraud Act, 9 V.S.A. § 2451, *et seq*.;

UU. the Virginia Consumer Protection Act of 1977, VA ST § 59.1-196, *et seq*.;

VV. the Washington Consumer Protection Act, RCWA 19.86.010, *et seq*.;

WW. the West Virginia Consumer Credit And Protection Act, W.Va.Code § 46A-1-101, *et seq*.;

XX. the Wisconsin Deceptive Trade Practices Act, WIS.STAT. § 100.18, *et seq*.; and

YY. the Wyoming Consumer Protection Act, WY ST § 40-12-101, *et seq*.

168. Defendant wrongfully and deceitfully collects consumer data in the course of its business transactions with consumers by telling consumers they must physically turn over to a Target employee their Driver's License as a condition precedent to a transaction.

169. Upon receiving a consumer's driver's license, Defendant requires its employees to swipe the consumer's Driver's License through a reader as described above to capture the information on that driving record.

170. Defendant engaged, and still engages in, unfair or deceptive acts or practices when it wrongfully and deceitfully collects consumer data, and misrepresents its reasons for requiring customers to hand over their driver's licenses.

171. Defendant intended, and still intends, that Plaintiffs and the members of the Class rely upon Defendant's misrepresentations and omissions concerning its reasons for requiring customers to hand over their driver's licenses.

172. Defendant does not inform a consumer that it is collecting this driver's data.

173. Defendant does not get written authorization from a consumer to collect this driver's data.

174. Defendant keeps said data for purposes outside of transaction verification, and

much longer than could be reasonably expected from Defendant's stated purpose of age verification.

175. Defendant's misrepresentations and omissions possess the tendency or capacity to mislead and create the likelihood of deception.

176. Plaintiffs and the Class had a reasonable right to rely on the veracity of Defendant's statements and did so in turning over their Drivers Licenses.

177. The above-described deceptive and unfair acts and practices were used or employed in the conduct of trade or commerce, namely, the everyday purchases of consumers at Defendant's stores by Plaintiffs and the Class members.

178. The above-described deceptive and unfair acts offend public policy and cause substantial injury to consumers.

179. Acting as reasonable consumers, had Plaintiffs and the Class known that their driver's licenses did not need to be physically turned over to Defendant for the stated purpose of age or identity verification, they would not have done so.

180. Acting as reasonable consumers, had Plaintiffs and the Class known that once physically turned over to Defendant that the personally identifiable information stored on that driver's record would be taken by Defendant by swiping their driver's licenses, they would not have physically turned them over.

181. As a direct and proximate result of these unfair, deceptive and unconscionable commercial practices, Plaintiffs and the members of the Class have suffered damages in the form invasion of privacy, breach of the covenant of fair dealing, and various federal and state statutes regarding driver's records.

182. The use and sale to third parties of this information caused harm to Plaintiffs and

the Class by, without permission or knowledge of Plaintiffs and the Class, influencing credit companies, health, and insurance companies.

183. Plaintiffs and the Class are burdened as well by marketing entities that now deluge Plaintiffs and the Class with unwanted advertising.

184. Therefore, Defendant engaged in a deceptive practice against consumers, causing consumers quantifiable harm and damages.

185. Plaintiffs, individually, and on behalf of the Class, seek statutory damages, and punitive damages, along with reasonable attorney's fees and costs.

186. Due to Defendant's misrepresentations and omissions described above,

187. Plaintiffs, individually, and on behalf of the Class, also seek injunctive relief. Plaintiffs seek an order:

a. requiring Defendant cease the deceptive scanning of driver's licenses described herein;

b. requiring Defendant inform Plaintiffs and the Class of the use of their driver's record information by third parties; and

c. requiring Defendant to remove the deceptively gotten information from its databases and records.

JURY TRIAL DEMAND

Pursuant to Fed. R. Civ. P. 38(b), Plaintiffs demand a trial by jury of all the claims asserted.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs and the proposed class members request that the Court enter an order or judgment against Defendant including the following:

A. Certification of the action under the Federal Rules of Civil Procedure 23 (b)(2), (b)(3) and (c)(4), and appointment of Plaintiffs as Class Representatives and their counsel of record as Class Counsel;

B. Statutory damages and such other relief as provided by the statutes cited herein;

C. Prejudgment and post-judgment interest on such monetary relief;

D. Equitable relief in the form of restitution and/or disgorgement of all unlawful or illegal profits received by Defendant as a result of the unfair, unlawful, and/or deceptive conduct alleged herein;

E. Equitable relief in the form of an injunction in that unless Defendant's unlawful practices are enjoined, Plaintiffs and the Class will continue to suffer irreparable injury; to this extent, their remedy at law is inadequate, and they are entitled to injunctive and other equitable relief herein requested;

F. The costs of bringing this suit, including reasonable attorneys' fees; and

G. All other relief to which Plaintiffs and Class Members may be entitled at law or in equity.

Dated: August 11, 2016
Manhasset, New York

Paul C. Whalen (PW-1300)
Law Office of Paul C. Whalen, P.C.
768 Plandome Road
Manhasset, NY 11030
Telephone: (516) 426-6870
paul@paulwhalen.com

Glancy Prongay & Murray LLP
Brian P. Murray
122 East 42nd Street, Suite 2920
New York, NY 10168
Telephone: (212) 682-5340
Email: bmurray@glancylaw.com

Jones Ward PLC
Jasper D. Ward IV
(*pro hac vice* application to be submitted)
312 S. Fourth Street
Louisville, KY 40202
Telephone: (502) 882-6000
jasper@jonesward.com

Morgan & Morgan
Complex Litigation Group
John A. Yanchunis
(*pro hac vice* application to be submitted)
201 North Franklin Street, 7th Floor
Tampa, FL 33602
Telephone: (813) 223-5505

Attorneys for Plaintiffs and the proposed Class